

UNITED STATES DISTRICT COURT

for the
Western District of New York

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Premises located at 382 Fielding Rd, Rochester, NY
14626, as described in Attachment A

Case No. 24-MJ-4035

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Premises located at 382 Fielding Rd, Rochester, NY 14626, as particularly described in Attachment A.

located in the Western District of New York, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, Items to be Seized and Searched, all of which are evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(2)(A) and (a)(5)(B).

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252A(a)(2)(A)	Receipt/Distribution of Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:

See attached affidavit of Federal Bureau of Investigations (FBI) Task Force Officer (TFO) Christopher Toscano, incorporated by reference herein.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Application submitted electronically by email in .pdf format. Oath administered and contents and signature attested to me as true and accurate telephonically pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on this 8th day of March, 2024.

City and state: Rochester, New York



Applicant's signature

Christopher Toscano, FBI TFO

Printed name and title



Judge's signature

Hon. Mark W. Pedersen, U.S. Magistrate Judge

Printed name and title

Type text here

ATTACHMENT A

DESCRIPTION OF PLACES AND ITEMS TO BE SEARCHED

The places and items to be searched are (A) the property located at 382 Fielding Road, Rochester, NY 14626 (the SUBJECT PREMISES), and (B) any computers, cellular telephones, tablets, computer equipment, computer storage media and electronic storage media found during said searches.

The SUBJECT PREMISES is depicted below and described as a single-family residence. The residence has white-colored siding with black shutters. Address number “382” is affixed to the mailbox next to the driveway of the residence.



ATTACHMENT B
ITEMS TO BE SEIZED AND SEARCHED

Evidence, in any form, electronic or otherwise, of violations of 18 U.S.C. §§ 2252A(a)(2)(A) (distribution/receipt of child pornography) and 2252A(a)(5)(B) (possession of child pornography).

1. Images of child pornography and files containing images of child pornography in any form, wherever they may be stored or found, including but not limited to: on any computer, phone, camera, tablet, disc, thumb drive, hard drive, or any other electronic data storage device;
2. Information, correspondence, communications, and other materials constituting evidence of, or pertaining to, a sexual interest in minors, wherever these items may be stored or found including on any computer, phone, camera, tablet, disc, thumb drive, hard drive, or any other electronic data storage device;
3. Any and all records, documents, e-mails, telephone numbers, text messages (in electronic or hardcopy), correspondence, communications, images, internet search history, or other information, which evince a sexual interest in minors or child exploitation;
4. Records and information relating to the existence of internet sites, social media applications, file sharing applications, or chat applications, related to child pornography or a sexual interest in children;
5. Documents and records, in any form or format, regarding the identity of any person using the identities: North Greece, kealedi_nkq_womdanso, Kealedi Angel Akter, any usernames assigned to Facebook User ID 61553191400565 (FB ACCOUNT 1), any usernames assigned to Instagram User ID 40920862467.
6. Records or other items related to the use of internet accounts, to include usernames, passwords, financial accounts, social media accounts, location information, IP information, etc., or any other information which evinces ownership or use of any digital equipment seized; and
7. Records, in whatever form, pertaining to residency at SUBJECT PREMISES and use or ownership of devices seized.

During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to obtain from GREGORY PUM (but

not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any devices requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person's physical biometric characteristics will unlock the devices, to include pressing finger(s) or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of:

- (a) any of the devices found at the PREMISES,
- (b) where the devices are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offenses as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the device's security features in order to search the contents as authorized by this warrant.

While attempting to unlock the device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the aforementioned person state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the device. Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned

person is permitted. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person for the password to any devices, or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any devices, the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, CHRISTOPHER TOSCANO, being duly sworn, depose and state:

1. I am a Deputy with the Monroe County Sheriff's Office and have been assigned as a Task Force Officer (TFO) with the FBI's Child Exploitation and Human Trafficking Task Force since 2017. As a TFO, I am responsible for investigating the production, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251(a), 2252A(a)(2)(A), and 2252A(a)(5)(B). I have been involved in hundreds of federal child pornography investigations and have seen thousands of images of child pornography as defined by 18 U.S.C. § 2256(8).

2. The information contained in this affidavit is based upon my personal knowledge and observations, my training and experience, conversations with other law enforcement officers, and my review of documents and records related to this case.

3. This affidavit is made in support of an application for a warrant to search the entire premises located at **382 Fielding Road, Rochester, New York (the "SUBJECT PREMISES")**, as more fully described and depicted in Attachment A, to include any computers, cellular telephones, tablets, computer equipment, computer storage media, and electronic storage media located therein.

4. As set forth in more detail below, there is probable cause to believe that evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2)(A) (distribution/receipt of child pornography) and Title 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography) (the "TARGET OFFENSES"), as more particularly described in Attachment B, are presently located at the SUBJECT PREMISES,

and on any computers, cellular telephones, tablets, computer equipment, computer storage media, and electronic storage media located therein or thereon.

5. Since this affidavit is being submitted for the limited purpose of establishing probable cause to secure a search warrant, I have not included every fact known to me concerning this investigation. Rather, I have set forth facts that I believe are relevant to establish probable cause to support the requested search warrant.

NCMEC CYBERTIPLINE

6. The National Center for Missing and Exploited Children (NCMEC) is a nonprofit organization that operates a “CyberTipline” through which internet and electronic service providers (ESPs) are required to report the presence of child pornography on their platforms. The duties of ESPs and NCMEC to report child exploitation and child pornography are set forth in 18 U.S.C. § 2258A.

7. If NCMEC receives a child exploitation Cybertip, it utilizes information provided by the ESP to determine the general geographic area (such as the state) where the offender is located. NCMEC then forwards the tip to law enforcement for further investigation on the information provided in the Cybertipline report.

FACEBOOK

8. Facebook is a social networking site that is owned and operated by Meta Platforms Inc. Facebook allows users to sign-up and create a free profile to connect and interact with other individuals. One-way users interact with one another is through the use

of Facebook Messenger. Facebook Messenger allows users to send messages, photographs, and videos, thus in and affecting interstate and foreign commerce via the internet.

SUMMARY OF PROBABLE CAUSE

9. As detailed below, two NCMEC Cybertipline reports were received reporting that (1) child pornography was uploaded by a Facebook Account on December 28, 2023, from an IP address associated with the SUBJECT PREMISES, and (2) suspected child pornography was uploaded by an Instagram Account on February 1, 2024 from the same IP address associated with the SUBJECT PREMISES. Based on the information below, I submit there is probable cause to believe that evidence of the possession, receipt, and distribution of child pornography will be located at the SUBJECT PREMISES. Additionally, I believe there is probable cause to believe that Gregory Pum, a registered sex offender who is on federal pretrial supervision for possessing child pornography, will be in possession of devices that have been used to possess, receive, and/or distribute child pornography.

PROBABLE CAUSE

10. On December 31, 2023, Facebook sent **Cybertipline Report 183378675** to NCMEC and listed the Incident Type¹ as “Child Pornography” (possession, manufacture,

¹ NCMEC Incident Type is based on a “Hash Match” of one or more uploaded files or NCMEC’s review of the report. “Hash matching” is a technological process through which an ESP can match an image or video to identical images or videos previously confirmed to depict child pornography as defined by 18 U.S.C § 2256(8). NCMEC may not have viewed all uploaded files submitted by the reporting ESP.

and distribution).” The report was processed by NCMEC on December 31, 2023, and provided to law enforcement.

11. The report for **183378675** provided the following information regarding the Facebook user being reported:

Name: North Greece
Mobile Phone: +1585XXX4865 (Verified) (hereinafter “MOBILE PHONE 1”)
ESP User ID: 61553191400565 (hereinafter “FB ACCOUNT 1”)
Profile URL: <https://www.facebook.com/profile.php?id=61553191400565>

12. The report for **183378675** stated that the FB ACCOUNT 1 uploaded one file on December 28, 2023, at 17:26:23 UTC from IP address 68.172.160.213 (IP ADDRESS 1). Facebook further provided messages captured around the time of the uploaded file.

- a. FB ACCOUNT 1 – “So good”
- b. ESP User ID 61552154855677 – “oh yea so good you’re nice they are doing good young girls”
- c. FB ACCOUNT 1 – “Eating out little vagina is good”

13. In the Cybertipline Report, Facebook stated that they did not view the entire contents of the uploaded file but categorized the image as “A2.” According to the categorization category, A2 is designated as “Prepubescent Minor” with “Lascivious Exhibition.” A further definition provided is as follows, “Any imagery depicting the lascivious exhibition of the anus, genitals, or pubic area of any person, where a minor is engaging in the lascivious exhibition or being used in connection with sexually explicit conduct, which may include but is not limited to imagery where the focal point is on the child’s anus, genitals, or pubic area and where the depiction is intended or designed to elicit a sexual response in the viewer.”

CYBERTIPLINE REPORT SEARCH WARRANT

14. On February 27, 2024, a search warrant was signed by U.S. Magistrate Judge Mark W. Pedersen authorizing the search of the associated files provided in the Cybertipline Report 183378675. That same day, your affiant executed the signed search warrant by reviewing the associated file and describes this file as follows:

File Name:
DPRpXW3NAcsbqu1O410952240_733342335524153_7005979456806746897_m.jpg

Description: An image depicting a prepubescent age girl naked with her vagina exposed in a lascivious manner. The prepubescent girl is kneeling with her legs spread open so her vagina is completely exposed, and appears to be the prominent focal point of the image. Furthermore, the image appears to be photomontage. Approximately five minor age children's faces are placed at the bottom of the image while two other individuals appear on either side of the prepubescent girl. Additionally, the image contains text appearing to be typed onto the image. The text observed contains the following, "New unique collection that contains thousands of ex-clusive uncensored Lolita images can grant you perhaps the best pleasure of your lifetime.", "We offer EXCLUSIVE Images and videos of all-time best Lolita beauties online sale! Best lola photographers have joined their efforts to create the collection of images completely of a different level! You can buy them only on this site. All material are exclusive." And "All the images are uncensored and were made with parental permission."

Based on my training and experience, I believe that this image constitutes child pornography as defined by 18 U.S.C § 2256(8).

T-MOBILE SUBPOENA

15. An FBI office subpoenaed T-Mobile for MOBILE PHONE 1. T-Mobile returned with the following subscriber information:

K[redacted] H[redacted]
190 [Redacted]
Rochester, NY 14616²

² These records are redacted to protect the identity of this individual.

CHARTER COMMUNICATIONS SUBPOENA

16. An FBI office subpoenaed Charter Communications for IP ADDRESS 1 (68.172.160.213). Charter Communications returned with the following subscriber information:

Sharon Pum³
382 Fielding Road
Rochester, NY 14626
Lease Log: Start Date 11/04/2022 End Date 02/24/2024⁴

OPEN-SOURCE SEARCH

17. Open-source research was conducted on FB ACCOUNT 1. On January 12, 2024, and January 25, 2024, FB ACCOUNT 1 posted a link to the Instagram account “kealedi_nkq__womdanso” (hereinafter “INSTAGRAM ACCOUNT 1”).

18. Your affiant conducted open-source research on INSTAGRAM ACCOUNT 1 on or about March 5, 2024, and observed the following.

19. INSTAGRAM ACCOUNT 1 had the same profile picture as FB ACCOUNT 1.

20. INSTAGRAM ACCOUNT 1 posted several photographs and videos that depicted minor age children in various settings that would constitute child erotica.

21. INSTAGRAM ACCOUNT 1’s profile also had a link for a Telegram channel. The Telegram channel had an image depicting a clothed minor child. A description of this channel indicated the following, “Absolutely no Negative. No spam. Nothing illegal. Love

³ Sharon Pum is Gregory Pum’s mother.

⁴ According to Charter Communications, this lease log information reflects that IP ADDRESS 1 was assigned to that subscriber during the period between 11/04/22 and 02/24/2024. It does not mean that service terminated after 02/24/2024 or that the IP ADDRESS was *not* assigned to that subscriber after 02/24/2024.

with empathy.” To date, there appear to have been approximately 43 photos, 216 videos, 1 file, 334 shared links, and 6 GIFS posted within this channel. A majority of the content posted within this channel appears to depict child erotica.

META PLATFORMS INC. SUBPOENAS

22. An FBI office subpoenaed Meta Platforms Inc. for the FB ACCOUNT 1 and INSTAGRAM ACCOUNT 1. Meta Platforms Inc. provided the following information on or about February 27, 2024.

23. Meta Platforms Inc. returned the following subscriber information:

a) FACEBOOK ACCOUNT 1

ESP User ID 61553191400565

Registration Date: 2023-10-31 05:20:32 UTC

Registration IP: 68.172.160.213 (IP ADDRESS 1)

Phone Number: 585-XXX-4865⁵ Cell Verified on 2023-10-31 05:20:53 UTC

Logins:

- IP Address 68.172.160.213 (IP ADDRESS 1)
Time – 2024-01-11 05:12:30 UTC
- IP Address 68.172.160.213 (IP ADDRESS 1)
Time – 2023-10-31 05:41:00 UTC
- IP Address 68.172.160.213 (IP ADDRESS 1)
Time – 2023-10-31 05:20:37 UTC

b) INSTAGRAM ACCOUNT 1

kealedi_nkq_womdanso

ESP User ID – 40920862467

Registration Date – 2020-09-02 14:09:03 UTC

Registration IP – 172.101.160.62

Phone Number – 716-640-8055 Cell Verified⁶ (hereinafter MOBILE PHONE 2)

⁵ MOBILE PHONE 1.

⁶ Instagram did not provide a date on which the cell phone number was verified.

24. Utilizing a tool available to law enforcement, MOBILE PHONE 2 was preliminarily identified as belonging to Gregory Pum with an address of 382 Fielding Road in February 2024.

25. As to INSTAGRAM ACCOUNT 1, Meta Platforms Inc. provided login information at the time the account was logged into, including IP addresses. Your affiant observed approximately five different IP addresses associated with this account. Of the five observed IP addresses, the most frequently listed was IP ADDRESS 1 (subscribed to Sharon Pum at 382 Fielding Road, Rochester, NY.) According to Meta Platforms Inc., INSTAGRAM ACCOUNT 1 was logged into from IP ADDRESS 1 as recently as February 24, 2024. Additionally, one of the IP addresses utilized to log into the Instagram account appears to be a VPN.

26. Additionally, Meta Platforms Inc., indicated that a CyberTip, ID 186300138, had been submitted associated with INSTAGRAM ACCOUNT 1, which is discussed below.

CYBERTIPLINE REPORT 186300138
REGARDING INSTAGRAM ACCOUNT 1

27. On February 4, 2024, Instagram sent **Cybertipline Report 186300138** to NCMEC and listed the Incident Type as “Child Pornography” (possession, manufacture, and distribution).” The report was processed by NCMEC on February 4, 2024, and provided to law enforcement.

28. The report for **186300138** provided the following information regarding the Instagram user being reported:

Name: Kealeddi Angel Akter
Mobile Phone: +7166408055 (Verified)

Email Address: sarsar4748@gmail.com (Verified)

Email Address: greg8548@gmail.com

Screen/User Name: kealedi_nkq__womdanso

ESP User ID: 40920862467

Profile URL: <https://www.instagram.com/uid/40920862467>

29. The report for **186300138** stated that INSTAGRAM ACCOUNT 1 uploaded one file on February 1, 2024, at 22:47:57 UTC from IP address 68.172.160.213 (IP ADDRESS 1).

30. The report indicated, “[a]ctivity on the platform indicates that the user is a minor, despite their listed age being an adult.”⁷

31. In the Cybertipline Report, Instagram stated that they did not view the entire contents of the uploaded file but categorized the image as “B1” and tagged as “Potential Meme.” According to the categorization category, B1 is designated as “Pubescent Minor” with “Sex Act.” A further definition provided is as follows, “[a]ny imagery depicting sexual intercourse (including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction of the above that lacks serious literary, artistic political, or scientific value.”

⁷ In my experience and training, I have seen subjects take on the persona of a minor online to engage with actual minors.

IDENTIFICATION OF GREGORY PUM

32. In January 2014, Gregory PUM was convicted of Possessing a Sexual Performance by a Child less than 16 years of Age and was sentenced to 10 years' probation and designated as a level 1 sex offender.

33. On or about January 23, 2023, PUM was charged Federally by criminal complaint with receipt and possession of child pornography stemming from an investigation related to CyberTipline Reports submitted to NCEMC. PUM is currently on pre-trial release.

34. On February 16, 2024, the Greece Police Department (GPD) made contact with PUM to interview him as a person with knowledge involving a burglary investigation. PUM identified living at 382 Fielding Road.

GREECE POLICE INVESTIATION

35. Your affiant was made aware of an ongoing police investigation involving PUM, and the report of a past sexual contact with a child. Through GPD's investigation, they learned that PUM is known to the child and the child's mother. That mother is the same person as K[redacted] H[redacted] (CW1) as indicated in paragraph 15 above.

36. GPD spoke with CW1 on February 28, 2024. According to CW1, she has never been to PUM's current residence and when asked stated 585-XXX-4865 (MOBILE PHONE 1) is the number she has saved in her phone for PUM.

TRAINING AND EXPERIENCE

37. Based on my training and experience, individuals who engage in the elicitation of child pornography often store and maintain images, records, and communications relating

to this illegal activity and often keep communications with other like-minded individuals saved in accounts.

38. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt/distribution and possession of child pornography:

- a. Those who receive and attempt to receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- b. Those who receive/distribute and possess child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videos, books, slides and/or drawings or other visual media. Such individuals often use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual act.
- c. Those who receive/distribute and possess child pornography often possess and maintain their “hard copies” of child pornographic material, that is, their pictures, films, videos, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals sometimes retain pictures, films, videos, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, and child erotica for many years.
- d. Likewise, those who receive/distribute and possess child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer, or other digital device, and surrounding area. These collections are often maintained for several years and are kept close by, to enable the collector to view the collection, which is valued highly. In many cases, the individual may try to hide the collection or may use a computer, such as a laptop, that can easily be transported from one location to another, in order to keep his collection private and not make it known

to other individuals he or she may be residing with. One method of transportation includes but is not limited to, the use of vehicles.

- e. Those who receive/distribute and possess child pornography also may correspond with and/or meet others to share information and materials; often maintain correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of individuals with whom they have been in contact and who share the same interests in child pornography. Those who distribute and possess child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
- f. Files of child pornography stored on digital devices, such as thumb drives, can sometimes be viewed by law enforcement even after having been deleted.
- g. Files of child pornography stored on digital devices are often copied onto other digital storage media, such as thumb drives, computers, or external hard drives, by those engaged with the child pornography activity.

SPECIFICS REGARDING A COMPUTER SEIZURE AND SEARCH

39. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, and memory chips. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B). I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

- a. Searching computer systems is a highly technical process which requires

specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a complete search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

- b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.
- c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of a premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text.
- d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

BIOMETRIC ACCESS TO DEVICES

40. This warrant permits law enforcement agents to obtain from the person of GREGORY PUM (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any devices requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person's physical biometric characteristics will unlock the device. The grounds for this request are as follows.

41. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

42. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

43. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain devices including those manufactured by Android, Apple, or other manufacturers. In many cases, a user registers for this feature by holding the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face.

44. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

45. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

46. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

47. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

48. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any devices, including to (1) press or swipe the finger(s) (including thumbs) of the aforementioned person to the

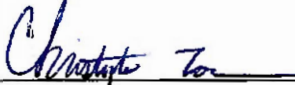
fingerprint scanner of the devices found at the PREMISES; (2) hold the devices found at the PREMISES in front of the face of the aforementioned person to activate the facial recognition feature; and/or (3) hold the devices found at the PREMISES in front of the face of the aforementioned person to activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.

49. The proposed warrant does not authorize law enforcement to require that the aforementioned person state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices. Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person for the password to any devices, or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any devices the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.


CONCLUSION

50. Based upon the forgoing, I respectfully submit that there is probable cause to believe that evidence, contraband, fruits, and instrumentalities of the TARGET OFFENSES, as specifically described in Attachment B to this application, are presently located within the SUBJECT PREMISES, as further described and depicted in Attachment A.

51. Due to the ongoing nature of this investigation, and the possibility of seriously jeopardizing the effectiveness of the investigation if information were made public, I request that the search and seizure warrant, and this application be sealed until further order of the Court.


CHRISTOPHER TOSCANO
Task Force Officer
Federal Bureau of Investigation

Affidavit submitted electronically by email in .pdf format. Oath administered, and contents and signature attested to me as true and accurate telephonically pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on March 8, 2024.


HON. MARK W. PEDERSEN
United States Magistrate Judge